Instytut Matematyki
Wydział Matematyki i Informatyki
Uniwersytet Jagielloński

Złamanie szyfru Enigmy przy użyciu teorii permutacji

Joanna Wąsik

Praca magisterska pod kierunkiem
prof. dr. hab. Zbigniewa Błockiego

Kraków, 2009

Spis treści

Przedmowa

Od zakończenia II Wojny Światowej minęło już ponad 60 lat, pomimo to niektóre fakty dotyczące jej przebiegu pozostają nieznane lub niejasne zarówno dla historyków jak i zwykłych ludzi. Podobnie jest z zasługami Polaków na polu działań wojennych, a w szczególności z ich wkładem w złamanie szyfru Enigmy. Ważne więc jest popularyzowanie prawdziwej historii polskich matematyków i ich osiągnięć. Nieliczne omówienia tematu opisujące metody wykorzystujące teorię permutacji, nie zawsze są przedstawiane w wyczerpujący sposób. Niniejsze opracowanie ma na celu zebranie dostępnych informacji i przedstawienie matematycznych obliczeń przeprowadzonych przez Mariana Rejewskiego, Jerzego Różyckiego i Henryka Zygalskiego (por. [3], [4]).

Pierwszy rozdział poświęcony jest przypomnieniu najważniejszych definicji z zakresu teorii permutacji, przytoczonych za książką Jerzego Rutkowskiego [8]. Wiadomości te są wykorzystane w obliczeniach w dalszych częściach pracy.

Rozdział drugi opisuje budowę maszyny szyfrującej Enigma (zobrazowanej schematycznym rysunkiem pochodzącym z *Wiadomości matematycznych* [4]) i sposób jej działania.

Kolejna część pracy przedstawia poszczególne etapy rozkodowania szyfru przy użyciu permutacji i twierdzeń z nimi związanych. Odpowiednie przykłady (por. [3], [4]) obrazują wykorzystanie osiągniętych wyników w praktyce.

Ostatnie dwa rozdziały opisują najważniejsze usprawnienia, wprowadzone przez matematyków do procesu odtwarzania poszukiwanych kluczy, mające na celu szybkie odczytywanie niemieckich depesz. Zarówno załączony przykład (por. [2]) jak i rysunki (pochodzące z [2] i [5]) przybliżają posługiwanie się wynalezionymi metodami.

Pragnę złożyć podziękowania Panu Profesorowi Zbigniewowi Błockiemu za poświęcony czas oraz cenne uwagi przy pisaniu pracy.

1 Podstawowe pojęcia

Definicja 1.1 *Każde wzajemnie jednoznaczne przekształcenie zbioru skończonego $X = \{a_1, \ldots, a_n\}$ na siebie nazywamy permutacją.*

Ponieważ elementy zbioru skończonego można ponumerować i utożsamiać je z ich numerami, można więc ograniczyć się do rozpatrywania permutacji zbioru $X = \{1, \ldots, n\}$ dla $n \in \mathbb{N}$.

Definicja 1.2 *Grupę permutacji zbioru $\{1, \ldots, n\}$ nazywamy grupą symetryczną stopnia n i oznaczamy symbolem S_n.*

Definicja 1.3 *Permutację $\tau \in S_n$ nazywamy cyklem o długości k, jeśli istnieje podzbiór $A = \{a_1, \ldots, a_k\}$ zbioru $\{a_1, \ldots, a_n\}$ taki, że $\tau(a_1) = a_2$, $\tau(a_2) = a_3$, ..., $\tau(a_{k-1}) = a_k$, $\tau(a_k) = a_1$ oraz $\tau(a_i) = a_i$ dla $a_i \notin A$. Wtedy τ zapisujemy w postaci $(a_1, \ldots, a_k)$.*

Permutacja identycznościowa jest cyklem o długości 1 i oznaczamy ją symbolem *id* lub (1).

Definicja 1.4 *Transpozycja jest to cykl dwuwyrazowy.*

Definicja 1.5 *Cykle $(a_1, \ldots, a_k), (b_1, \ldots, b_l) \in S_n$ nazywamy cyklami rozłącznymi, jeśli rozłączne są zbiory $\{a_1, \ldots, a_k\}$ i $\{b_1, \ldots, b_l\}$.*

Fakt 1.6 *Każdą permutację można przedstawić w postaci iloczynu cykli rozłącznych. Dowolny cykl $(a_1, \ldots, a_k) \in S_n$ rozkłada się na iloczyn transpozycji według wzoru:*

$$(a_1, a_2, \ldots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \ldots (a_1, a_2).$$

Rozkład permutacji $\tau \in S_n$ na iloczyn transpozycji nie jest jednoznaczny. Parzystość liczby transpozycji w rozkładach nie zależy jednak od tych rozkładów, a jedynie od samej permutacji.

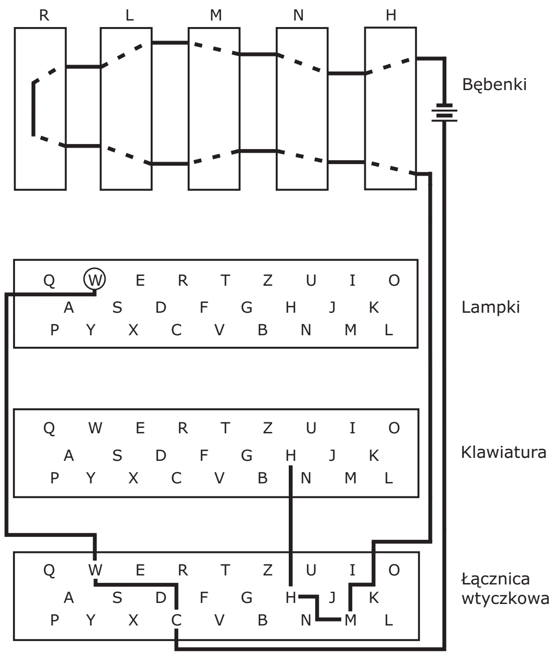
Definicja 1.7 *Znakiem permutacji nazywamy liczbę $sgn\tau$ określoną wzorem:*

$$sgn\tau = \begin{cases} 1, & \text{jeśli } \tau \text{ jest parzysta;} \\ -1, & \text{jeśli } \tau \text{ jest nieparzysta.} \end{cases}$$

2 Konstrukcja i działanie Enigmy

Enigma wojskowa była wielkości maszyny do pisania i posiadała 26-literową klawiaturę. W górnej jej części, zamiast czcionek, umieszczona była płytka z 26 podświetlanymi literami. Główną częścią maszyny były: nieruchomy walec wstępny H, trzy współosiowe, wzajemnie przestawialne wirniki szyfrujące N, M, L oraz walec odwracający R. Bębenki N, M, L posiadały pierścienie, na których obwodzie umieszczone były litery alfabetu. Wewnątrz pierścieni znajdowały się kontakty stałe oraz kontakty sprężynujące, połączone ze sobą w nieregularny sposób. Walec odwracający posiadał tylko z jednej strony kontakty sprężynujące, połączone nieregularnie parami. Z przodu urządzenia znajdowała się łącznica wtyczkowa S, umożliwiająca zamianę dowolnych 6 par liter.

Permutacje dokonane za pomocą bębenków N, M, L oraz H były identyczne w każdej Enigmie danego typu. Permutacja R była taka sama jak R^{-1}, a permutacja S, w rozkładzie na cykle rozłączne, składała się z 6 transpozycji.



Rysunek 2.1: Schemat przepływu prądu w Enigmie.

Naciśnięcie jednego z klawiszy klawiatury powodowało przepływ prądu od łącznicy wtyczkowej przez wirniki szyfrujące, bębenek odwracający, ponownie przez łącznicę aż do żarówek. Za każdym naciśnięciem klawisza pierwszy wirnik obracał się o 1/26 kąta pełnego. Jednocześnie zapalała się żarówka podświetlająca literę, różną od naciśniętego klawisza. Po pełnym obrocie pierwszego wirnika obracał się drugi, a po obrocie drugiego również trzeci. Ze względu na rzadkie obroty tych wirników można je było pominąć w obliczeniach. Walec odwracający był nieruchomy. Dzięki temu Enigma służyła zarówno do szyfrowania tekstu otwartego, jak i do zamiany szyfru na kler.

Z budowy maszyny wynikało (rys. 2.1), że i-tą literę każdej depeszy przekształcała permutacja

$$A_i = S^{-1}H^{-1}P^{-i}N^{-1}P^{i}QP^{-i}NP^{i}HS, \qquad i = 1, 2, 3 \ldots, \qquad (2.1)$$

gdzie

$$Q = M^{-1}L^{-1}RLM,$$

a $P = (\,1\,2\,3 \ldots\ 24\,25\,26)$ była permutacją spowodowaną obrotem wirnika N (liczby oznaczały kolejne litery alfabetu).

Dzięki budowie bębenka R

$$A_i = A_i^{-1}.$$

3 Rozszyfrowanie Enigmy

3.1 Szyfrowanie i klucze depesz

Do jesieni 1938 roku w armii niemieckiej obowiązywały ustalone przepisy dotyczące kodowania depesz. Szyfrant sprawdzał, w tablicy kluczy dziennych, obowiązujące danego dnia ustawienie łącznicy wtyczkowej S oraz bębenków N, M, L. Następnie samodzielnie wybierał szyfr indywidualny α, β, γ dla każdej depeszy, po czym dwukrotnie go szyfrował. Otrzymane 6 liter umieszczał na początku przekazu. Później zmieniał nastawienie wirników na wybrany klucz indywidualny i nadawał właściwą wiadomość. Pierwszych sześć liter każdej depeszy było postaci:

$$A_1(\alpha), A_2(\beta), A_3(\gamma), A_4(\alpha), A_5(\beta), A_6(\gamma),$$

gdzie permutacje $A_1, \ldots, A_6$ były stałe danego dnia.

To, że pierwszych sześć liter każdej depeszy stanowiło jej trzyliterowy, dwukrotnie zaszyfrowany klucz było oczywiste. Jeśli bowiem w telegramach z danego dnia takie same były pierwsze litery to identyczne były czwarte, jeśli powtarzały się drugie to i piąte itd. Posiadając dostateczną liczbę wiadomości z danego dnia (około 80), kryptolog mógł odtworzyć iloczyny A_4A_1, A_5A_2, A_6A_3 postępując według ustalonego schematu. Z przechwyconych danego dnia depeszy wybierano dowolną, po czym zapisywano pierwszą literę. Obok pierwszej należało napisać czwartą literę zaszyfrowanego klucza. Następnie znajdowano depeszę zaczynającą się od czwartej z poprzedniej wiadomości. Przy niej zapisywano znów czwartą nowego szyfru. Dzięki temu powstawał cykl liter. Z niewykorzystanych jeszcze znaków powstawały kolejne cykle. Postępowanie powtarzano także dla drugich i piątych oraz trzecich i szóstych liter. Po rozpisaniu ich na cykle rozłączne okazało się, że wszystkie mają specyficzną własność:

cykle tej samej długości występują w liczbie parzystej.

Mimo, że obraz takiego układu zmieniał się każdego dnia, cecha była stale taka sama. Ze względu na rolę jaką ten układ pełnił nazwano go *charakterystyką* danego dnia. Następnie, aby ułatwić sobie pracę, sformułowano twierdzenia pomocnicze.

Twierdzenie 3.1 (O iloczynie transpozycji) *Jeśli dwie permutacje ρ i σ tego samego stopnia składają się z samych transpozycji rozłącznych, wtedy*

w ich iloczynie $\rho\sigma$ cykle rozłączne tej samej długości występują w liczbie parzystej.

Dowód. Niech ρ i σ będą permutacjami spełniającymi założenia twierdzenia. Oznaczmy ich stopień przez $2n$, gdzie $n \in \mathbb{N}$. Rozważamy następujące dwa przypadki:

1. W ρ i σ występuje taka sama transpozycja (ab).
   Wtedy w $\tau = \rho\sigma$ wystąpi para cykli jednoliterowych (a) i (b). Twierdzenie jest więc prawdziwe dla transpozycji identycznych w obu permutacjach.

2. Permutacje ρ i σ składają się z różnych transpozycji rozłącznych.

W permutacji ρ wystąpi	W permutacji σ wystąpi
(a_1a_2)	(a_2a_3)
(a_3a_4)	(a_4a_5)
$\vdots$	$\vdots$
$(a_{2k-3}a_{2k-2})$	$(a_{2k-2}a_{2k-1})$
$(a_{2k-1}a_{2k})$	$(a_{2k}a_1)$

ponieważ wyraz początkowy a_1 musi wystąpić w σ $(k \in \mathbb{N}, k \leqslant n)$.

Wtedy

$$\tau = \rho\sigma = (a_2a_4a_6 \dots a_{2k-2}a_{2k})(a_{2k-1}a_{2k-3} \dots a_5a_3a_1),$$

a otrzymane cykle mają taką samą długość równą k.

Jeśli w ten sposób nie zostały wykorzystane wszystkie wyrazy, kontynuujemy nasze postępowanie aż do ich wyczerpania.

□

Twierdzenie 3.2 (Odwrotne do twierdzenia o iloczynie transpozycji) *Jeżeli w permutacji parzystej τ, cykle rozłączne tej samej długości występują w liczbie parzystej, to wtedy istnieją permutacje ρ i σ złożone z samych transpozycji rozłącznych takie, że $\tau = \rho\sigma$.*

Dowód. Niech τ spełnia założenia twierdzenia. Permutację τ możemy przedstawić jako: $\tau = \tau_1 \dots \tau_n$, τ_i rozłączna z τ_j dla $i \neq j,\ i, j = 1, 2, \dots, n$, gdzie

$$\tau_i = (a_1 a_2 \dots a_{k_i})(b_1 b_2 \dots b_{k_i}), \qquad n, k_i \in \mathbb{N},\ i = 1, \dots, n.$$

Niech ρ_i i σ_i będą szukanymi rozkładami na transpozycje: $\tau_i = \rho_i \sigma_i$. Wystarczy wtedy zdefiniować je jako:

$$\sigma_i = (a_1 b_1)(a_2 b_{k_i})(a_3 b_{k_i - 1})(a_4 b_{k_i - 2}) \dots (a_{k_i - 2} b_4)(a_{k_i - 1} b_3)(a_{k_i} b_2),$$
$$\rho_i = (b_2 a_1)(b_1 a_2)(b_{k_i} a_3)(b_{k_i - 1} a_4) \dots (b_5 a_{k_i - 2})(b_4 a_{k_i - 1})(b_3 a_{k_i}).$$

Ponieważ każdą permutację τ_i da się przedstawić w tej postaci, więc τ można przedstawić jako:

$$\tau = \rho\sigma,$$

gdzie $\rho = \rho_1 \dots \rho_n$, $\sigma = \sigma_1 \dots \sigma_n$, $n \in \mathbb{N}$.

□

Stwierdzenie 3.3 *Litery wchodzące do jednej i tej samej transpozycji permutacji ρ lub σ, wchodzą zawsze do dwóch różnych cykli tej samej permutacji $\rho\sigma$.*

Korzystając z Twierdzenia 3.1 i Stwierdzenia 3.3 wyznaczano możliwe rozwiązania. Najpierw grupowano cykle tej samej długości k w pary. Następnie każdą parę należało przedstawić w postaci iloczynu dwóch permutacji, składających się z k transpozycji rozłącznych. W ten sposób otrzymywano od kilkunastu do kilkudziesięciu postaci każdej z permutacji A_1, A_2, A_3 (zależnie od wyglądu iloczynów $A_4 A_1$, $A_5 A_2$, $A_6 A_3$). Na cały układ istniało więc od kilkunastu tysięcy do kilkudziesięciu tysięcy rozwiązań, wśród których znalezienie właściwego było pracochłonne. W tej sytuacji pomocna okazała się znajomość nawyków szyfrantów, którzy jako klucz depeszy często wybierali trzy te same lub trzy sąsiadujące ze sobą na klawiaturze litery. Wykorzystując tę informację, ze zbioru rozwiązań wybierano to, które najczęściej dawało to samo α, β, γ.

Poniższy przykład przybliży metodę znajdowania permutacji $A_1, \dots, A_6$.

Przykład. Załóżmy, że dzięki dostatecznej liczbie wiadomości, mamy odtworzone charakterystyki:

$$\begin{aligned} A_4A_1 &= (dvpfkxgzyo)(eijmunglht)(bc)(rw)(a)(s), \\ A_5A_2 &= (blfqveoum)(hjpswizrn)(axt)(cgy)(d)(k), \\ A_6A_3 &= (abviktjgfcqny)(duzrehlxwpsmo). \end{aligned} \tag{3.1}$$

Wiemy też, że szyfranci wybierają jako klucze jednakowe litery np. aaa. W iloczynie A_4A_1 tylko a i s tworzą cykle jednoliterowe, więc jeśli wśród kluczy miał być klucz aaa, to po zaszyfrowaniu pierwszą literą powinna być s. Niech

$$\begin{matrix} sug & smf \\ sjm & spo \\ syx & scw \end{matrix}$$

będą trzema kluczami depesz z danego dnia. Klucz $sug\ smf$ nie powstał z aaa, ponieważ u i a znajdują się w dwóch cyklach różnej długości iloczynu A_5A_2. Podobnie szyfr $sjm\ spo$ nie mógł powstać z aaa. Klucz $syx\ scw$ mógł natomiast pochodzić od aaa. Litery a i s leżą w różnych cyklach jednoliterowych A_4A_1. Tak samo w A_5A_2, y i a są w różnych cyklach trzyliterowych, a także x i a należą do różnych cykli tej samej długości permutacji A_6A_3. Teraz można było w jednoznaczny sposób rozpisać A_3 i A_6:

$$\begin{aligned} A_3 &= (ax)(bl)(cm)(dg)(ei)(fo)(hv)(ju)(kr)(np)(sq)(tz)(wy), \\ A_6 &= (aw)(bx)(co)(df)(ek)(gu)(hi)(jz)(lv)(mq)(ns)(py)(rt). \end{aligned}$$

Na podstawie szyfru $syx\ scw$ udało się także wyznaczyć część transpozycji pozostałych permutacji:

$$\begin{aligned} A_1 &= (as)(br)(cw)(\ldots), \\ A_2 &= (ay)(ct)(dk)(gx)(\ldots), \\ A_4 &= (as)(bw)(cr)(\ldots), \\ A_5 &= (ac)(dk)(gt)(xy)(\ldots). \end{aligned}$$

Do odnalezienia pozostałych transpozycji potrzebne były kolejne szyfrogramy. Odczytywano je jako ciągi bbb, fff, co potwierdzało słuszność założenia, że $syx\ scw$ przed zaszyfrowaniem oznaczało właśnie aaa.

Pierwsza tajemnica Enigmy została więc odkryta. Co ważne, do jej rozwiązania nie była potrzebna ani wiedza o połączeniach elementów szyfrujących urządzenia, ani znajomość kluczy dziennych. Wystarczyła odpowiednia liczba wiadomości oraz znajomość zwyczajów szyfrantów. Kiedy na początku Rejewski założył, że klucze są złożone z jednakowych liter, była to tylko hipoteza. Przypuszczenie to szczęśliwie się sprawdziło. Od tego momentu dokładnie śledzono upodobania szyfrantów. I tak w momencie kiedy zabroniono im używać trzech identycznych liter, unikali powtórzenia się którejkolwiek lub używali liter sąsiadujących na klawiaturze. Zawsze udawało się jednak zauważyć schemat w postępowaniu Niemców, który stanowił punkt wyjścia do złamania szyfru.

Następnym zadaniem stojącym przed kryptologiem było odnalezienie połączeń wewnętrznych bębenków.

3.2 Połączenia wewnętrzne

Poważnym błędem Niemców było szyfrowanie kluczy depesz. Nie zabezpieczyło to ich przed rozkodowaniem, a dzięki charakterystykom 3.1 udało się odtworzyć czynniki A_i. Znajomość permutacji $A_1, \ldots, A_6$ ułatwiła odnalezienie połączeń wewnętrznych bębenków. Wykorzystano do tego równania 2.1. Pisząc je zakładano, że podczas używania Enigmy, obracał się tylko wirnik N. Sytuacja taka miała miejsce 21 na 26 razy, więc na tyle często, aby zapisać wzory w danej postaci. W celu znalezienia połączeń wewnętrznych bębenków, należało więc rozwiązać układ sześciu równań (2.1) z czterema niewiadomymi (S, H, N, Q):

$$A_i = S^{-1}H^{-1}P^{-i}N^{-1}P^{i}QP^{-i}NP^{i}HS, \qquad i = 1, \ldots, 6;$$

$$Q = M^{-1}L^{-1}RLM.$$

Starano się najpierw uprościć powyższe równania. Znając połączenia wewnętrzne wirnika wstępnego w handlowej Enigmie założono, że w wojskowej wersji będzie tak samo. Wiersz argumentów permutacji H przedstawiał alfabet w kolejności liter na klawiaturze:

$$H = \begin{pmatrix} q & w & e & r & t & z & u & i & o & a & s & d & f & g & h & j & k & p & y & x & c & v & b & n & m & l \\ a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \end{pmatrix}.$$

Teraz pozostał do rozwiązania układ sześciu równań z trzema niewiadomymi. Było to trudne zadanie, z którym nie potrafiono sobie poradzić aż

do grudnia 1932 roku. Wywiad francuski dostarczył wtedy fotokopię dwóch tablic kluczy dziennych za wrzesień i październik 1932 roku. Zawierała ona oprócz pozycji i kolejności wirników także ustawienia łącznicy. Dzięki temu można było uznać permutację S za znaną i razem z H przenieść na lewą stronę:

$$\begin{aligned}
HSA_1S^{-1}H^{-1} &= P^{-1}N^{-1}PQP^{-1}NP,\\
HSA_2S^{-1}H^{-1} &= P^{-2}N^{-1}P^2QP^{-2}NP^2,\\
&\vdots\\
HSA_6S^{-1}H^{-1} &= P^{-6}N^{-1}P^6QP^{-6}NP^6.
\end{aligned}$$

Znane, lewe strony oznaczono jako U_i, a każde z równań przemnożono lewostronnie przez P^i i prawostronnie przez P^{-i} dla $i = 1, \ldots, 6$:

$$\begin{aligned}
U_1 &= PHSA_1S^{-1}H^{-1}P^{-1} = N^{-1}PQP^{-1}N,\\
U_2 &= P^2HSA_2S^{-1}H^{-1}P^{-2} = N^{-1}P^2QP^{-2}N,\\
&\vdots\\
U_6 &= P^6HSA_6S^{-1}H^{-1}P^{-6} = N^{-1}P^6QP^{-6}N.
\end{aligned}$$

Następnie utworzono iloczyny:

$$\begin{aligned}
U_2U_1 &= N^{-1}P(QPQP^{-1})P^{-1}N,\\
U_3U_2 &= N^{-1}P^2(QPQP^{-1})P^{-2}N,\\
&\vdots\\
U_6U_5 &= N^{-1}P^5(QPQP^{-1})P^{-5}N.
\end{aligned}$$

Eliminując z równań wspólny czynnik $QPQP^{-1}$ do rozwiązania pozostał układ czterech równań z jedną niewiadomą $N^{-1}PN$:

$$\begin{aligned}
U_3U_2 &= N^{-1}PN(U_2U_1)N^{-1}P^{-1}N,\\
U_4U_3 &= N^{-1}PN(U_3U_2)N^{-1}P^{-1}N,\\
U_5U_4 &= N^{-1}PN(U_4U_3)N^{-1}P^{-1}N,\\
U_6U_5 &= N^{-1}PN(U_5U_4)N^{-1}P^{-1}N.
\end{aligned} \tag{3.2}$$

Ponieważ $N^{-1}P^{-1}N = (N^{-1}PN)^{-1}$ więc do rozwiązania powyższego problemu przeprowadzono teoretyczne rozważania i wyprowadzono pomocnicze wzory.

Załóżmy, że mamy dwie permutacje, niewiadomą ω oraz znaną ρ daną wzorem:

$$\rho = \begin{pmatrix} 1 & 2 & \dots & 26 \\ \rho(1) & \rho(2) & \dots & \rho(26) \end{pmatrix} = (a_1 a_2 \dots a_{k_1})(b_1 b_2 \dots b_{k_2}) \dots ,$$

gdzie $i, k_i \in \mathbb{N}$, $i \leqslant 26$, $\sum_i k_i = 26$.

Wtedy

$$\omega\rho\omega^{-1} = \begin{pmatrix} 1 & 2 & \dots & 26 \\ \omega(1) & \omega(2) & \dots & \omega(26) \end{pmatrix}(a_1 a_2 \dots a_{k_1})(b_1 b_2 \dots b_{k_2}) \dots$$

$$\dots \begin{pmatrix} \omega(1) & \omega(2) & \dots & \omega(26) \\ 1 & 2 & \dots & 26 \end{pmatrix} =$$

$$= (\omega(a_1)\omega(a_2) \dots \omega(a_{k_1}))(\omega(b_1)\omega(b_2) \dots \omega(b_{k_2})).$$

Dla danej permutacji $\sigma = \begin{pmatrix} 1 & 2 & \dots & 26 \\ \sigma(1) & \sigma(2) & \dots & \sigma(26) \end{pmatrix}$ zachodzi także warunek: istnieje rozwiązanie równania $\sigma = \omega\rho\omega^{-1} \iff \sigma$ i ρ są podobne. Oznacza to, że σ składa się z tej samej liczby cykli długości $k_1, k_2, \dots$, co permutacja ρ. Aby znaleźć szukane rozwiązanie ω, należy najpierw pogrupować cykle danej długości z σ i ρ w pary. Następnie istnieje k_i sposobów podpisania cyklu długości k_i z σ, pod elementami odpowiadającego cyklu z ρ :

$$\begin{pmatrix} a_1\, a_2 \dots a_{k_1} \\ a'_1\, a'_2 \dots a'_{k_1} \end{pmatrix}, \begin{pmatrix} a_1\, a_2 \dots a_{k_1} \\ a'_2\, a'_3 \dots a'_1 \end{pmatrix}, \begin{pmatrix} a_1\, a_2 \dots a_{k_1} \\ a'_3\, a'_4 \dots a'_2 \end{pmatrix} \dots$$

gdzie $\rho = (a_1 a_2 \dots a_{k_1})(b_1 b_2 \dots b_{k_2}) \dots$, a $\sigma = (a'_1 \dots a'_{k_1})(b'_1 \dots b'_{k_2}) \dots$. Tak samo należy rozpisać pozostałe cykle z permutacji.

W rozważanej przez kryptologów sytuacji do rozwiązania były cztery równania:

$$U_{i+2}U_{i+1} = N^{-1}PN(U_{i+1}U_i)N^{-1}P^{-1}N, \qquad i = 1, 2, 3, 4,$$

z jedną niewiadomą $N^{-1}PN$. Ponieważ U_3U_2 zostało przekształcone z U_2U_1 przez iloczyn $N^{-1}PN$, więc szukając rozwiązania należało podpisać U_3U_2 pod U_2U_1 na wszystkie możliwe sposoby. Porównując iloczyny okazało się jednak, że nie były one do siebie podobne i nie można było zastosować teorii

do odnalezienia szukanego wyrażenia $N^{-1}PN$. Ponawianie prób na charakterystykach z różnych dni także nie przyniosło oczekiwanych rezultatów. Wysunięto przypuszczenie, że przyczyną niepowodzeń mogło być błędne przekonanie o wyglądzie permutacji H. Założono więc, że walec wstępny realizuje przekształcenie identycznościowe. Wyprowadzono wzory 3.2 z nowymi danymi i tym razem hipoteza okazała się prawdziwa. Udało się przeprowadzić odpowiednie obliczenia i z pierwszego równania uzyskano kilkadziesiąt możliwości na szukane $N^{-1}PN$. Postępując według opisanej powyżej metody ze wzorem na U_4U_3, otrzymano kolejne rozwiązania. Wśród nich jedno było identyczne z rozwiązaniem równania na U_3U_2. Pozostałe dwa równania na U_5U_4 i U_6U_5 były już niepotrzebne.

Następnym krokiem w rozszyfrowaniu było odtworzenie permutacji N z iloczynu $N^{-1}PN$. Ponieważ P była znana, odnalezienie połączeń wewnętrznych wirnika było tylko zadaniem rachunkowym. Z 26-ciu wyników właściwy wybierano drogą doświadczalną.

Połączenia drugiego i trzeciego bębenka odnaleziono tą samą metodą. Materiały wywiadowcze zawierały bowiem dane z różnych kwartałów, w których na pozycji bębenka N znajdowały się także inne wirniki. Wyznaczenie permutacji R było już proste. Wystarczyło przekształcić wzór 2.1 i wykonać obliczenia w nim wskazane (pamiętając, że $H = Id$):

$$R = LMP^{-i}NP^{i}SA_iS^{-1}P^{-i}N^{-1}P^{i}M^{-1}L^{-1},$$

dla dowolnego $i = 1, \ldots, 6$.

Praktyczne zastosowanie metody odnajdywania połączeń wewnętrznych przybliży następujący przykład.

Przykład. Załóżmy, że dzięki dostatecznej liczbie depeszy, z charakterystyk 3.1 mamy odtworzone permutacje:

$$\begin{aligned}
A_1 &= (as)(br)(cw)(di)(ev)(fh)(gn)(jo)(kl)(my)(pt)(qx)(uz),\\
A_2 &= (ay)(bj)(ct)(dk)(ei)(fn)(gx)(hl)(mp)(ow)(qr)(su)(vz),\\
A_3 &= (ax)(bl)(cm)(dg)(ei)(fo)(hv)(ju)(kr)(np)(sq)(tz)(wy),\\
A_4 &= (as)(bw)(cr)(dj)(ep)(ft)(gq)(hk)(iv)(lx)(mo)(nz)(uy),\\
A_5 &= (ac)(bp)(dk)(ez)(fh)(gt)(io)(jl)(ms)(nq)(rv)(uw)(xy),\\
A_6 &= (aw)(bx)(co)(df)(ek)(gu)(hi)(jz)(lv)(mq)(ns)(py)(rt).
\end{aligned}$$

Znając P możemy także obliczyć jej potęgi, a także znamy zmiany dokonane

przez łącznicę wtyczkową S:

$$
\begin{aligned}
P &= (a\,b\,c\,d\,e\,f\,g\,h\,i\,j\,k\,l\,m\,n\,o\,p\,q\,r\,s\,t\,u\,v\,w\,x\,y\,z),\\
P^2 &= (a\,c\,e\,g\,i\,k\,m\,o\,q\,s\,u\,w\,y)(b\,d\,f\,h\,j\,l\,n\,p\,r\,t\,v\,x\,z),\\
&\vdots\\
S &= (ap)(bl)(cz)(fh)(jk)(qu).
\end{aligned}
$$

Wykonując odpowiednie działania obliczamy U_1, U_2, U_3, i U_4 (U_5 i U_6 nie będą potrzebne), a następnie tworzymy iloczyny $U_{i+2}U_{i+1}$:

$$
\begin{aligned}
U_1 &= (ax)(bu)(ck)(dr)(ej)(fw)(gi)(lp)(ms)(nz)(oh)(qt)(vy),\\
U_2 &= (ar)(bv)(co)(dh)(fl)(gk)(iz)(jp)(mn)(qy)(su)(tw)(xe),\\
U_3 &= (as)(bz)(cp)(dq)(eo)(fw)(gj)(hl)(iy)(kr)(mu)(nt)(vx),\\
U_4 &= (ap)(bf)(cu)(dv)(ei)(gr)(ho)(jn)(ky)(lx)(mz)(qs)(tw);
\end{aligned}
$$

$$
\begin{aligned}
U_2U_1 &= (a\,e\,p\,f\,t\,y\,b\,s\,n\,i\,k\,o\,d)\,(r\,h\,c\,g\,z\,m\,u\,v\,q\,w\,l\,j\,x),\\
U_3U_2 &= (a\,k\,j\,c\,e\,v\,z\,y\,d\,l\,w\,n\,u)\,(s\,m\,t\,f\,h\,q\,i\,b\,x\,o\,p\,g\,r),\\
U_4U_3 &= (a\,q\,v\,l\,o\,i\,k\,g\,n\,w\,b\,m\,c)\,(p\,u\,z\,f\,t\,j\,r\,y\,e\,h\,x\,d\,s).
\end{aligned}
$$

Iloczyny są do siebie podobne, więc aby znaleźć rozwiązanie $N^{-1}PN$ należy podpisać U_3U_2 pod U_2U_1 oraz U_4U_3 pod U_3U_2 na wszystkie możliwe sposoby. Jedno rozwiązanie jest wspólne dla obydwu iloczynów (jest to szukane $N^{-1}PN$):

$$
\begin{aligned}
U_2U_1 &= (a\,e\,p\,f\,t\,y\,b\,s\,n\,i\,k\,o\,d)\,(r\,h\,c\,g\,z\,m\,u\,v\,q\,w\,l\,j\,x),\\
U_3U_2 &= (y\,d\,l\,w\,n\,u\,a\,k\,j\,c\,e\,v\,z)\,(i\,b\,x\,o\,p\,g\,r\,s\,m\,t\,f\,h\,q);
\end{aligned}
$$

$$
\begin{aligned}
U_3U_2 &= (y\,d\,l\,w\,n\,u\,a\,k\,j\,c\,e\,v\,z)\,(i\,b\,x\,o\,p\,g\,r\,s\,m\,t\,f\,h\,q),\\
U_4U_3 &= (u\,z\,f\,t\,j\,r\,y\,e\,h\,x\,d\,s\,p)\,(c\,a\,q\,v\,l\,o\,i\,k\,g\,n\,w\,b\,m);
\end{aligned}
$$

$$
N^{-1}PN = (a\,y\,u\,r\,i\,c\,x\,q\,m\,g\,o\,v\,s\,k\,e\,d\,z\,p\,l\,f\,w\,t\,n\,j\,h\,b).
$$

Pod otrzymanym wyrażeniem na $N^{-1}PN$ podpisujemy z kolei permutację P. Uzyskane rozwiązania nie różnią się w istotny sposób od siebie. Jednym jest na przykład:

$$
N = \begin{pmatrix} a & y & u & r & i & c & x & q & m & g & o & v & s & k & e & d & z & p & l & f & w & t & n & j & h & b \\ a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \end{pmatrix}.
$$

Wybór innego ustawienia oznacza tylko różnicę w większym lub mniejszym skręceniu prawej strony w stosunku do lewej strony bębenka. Ustalenie właściwej pozycji, polega na próbie odczytania kilku wiadomości i dokonaniu takich zmian, aby w rezultacie otrzymać bezbłędne treści depesz.

W ten sam sposób ustalano moment, w którym następuje obrót wirników L i M. Proces ten ułatwiła kryptologom niemiecka instrukcja obsługi Enigmy, dostarczona przez Gustawa Bertranda razem z tablicami kluczy dziennych. Zamieszczono w nich przykładową wiadomość i autentyczny szyfrogram, zakodowany przy podanym kluczu dziennym. W następnych wydaniach przykład zakodowanej depeszy był już fikcyjny.

Złamanie szyfru Enigmy było możliwe dzięki wiedzy polskich kryptologów, ich abstrakcyjnemu myśleniu, ale także dzięki szczęściu. W niektórych sytuacjach bowiem wysuwano pewną hipotezę i zakładając, że jest prawdziwa prowadzono obliczenia. Tak było w przypadku równań 2.1. Do dziś nie wiadomo czy da się, w prosty sposób, rozwiązać ten układ bez znajomości permutacji S. Inne metody, uniezależnione od znajomości kluczy dziennych, wymagały dużego nakładu pracy i nie gwarantowały sukcesu. Dostarczenie materiałów wywiadowczych odegrało więc kluczową rolę w złamaniu szyfru.

4 Metoda rusztu, metoda zegara, cyklometr

Odtworzenie połączeń wewnętrznych Enigmy było wielkim osiągnięciem. Znajomość budowy maszyny nie była jednak czynnikiem wystarczającym do płynnego odczytywania depesz. Po przebudowaniu Enigmy handlowej na wojskową zlecono fabryce AVA, ściśle współpracującej z Biurem Szyfrów, wykonanie kilkunastu replik Enigm według wytycznych podanych przez Mariana Rejewskiego. Posiadając identyczne urządzenia szyfrujące jak armia niemiecka, należało znaleźć sposób na sprawne odnajdywanie bieżących kluczy dziennych. Problem, z którym należało sobie poradzić był więc odwrotny do pierwotnego. Poprzednio znając klucze dzienne z pewnego okresu, musiano odtworzyć połączenia wewnętrzne. Teraz szukano metod pozwalających na szybkie odczytywanie wiadomości.

4.1 Metoda rusztu

Ponieważ w początkowym okresie używania Enigmy, kolejność wirników w maszynie zmieniana była raz na kwartał, priorytetem było sprawne określanie nastawienia bębenków. Pomagała w tym, opracowana jako pierwsza, metoda rusztu. Wykorzystywała ona fakt, że łącznica wtyczkowa zamieniała tylko 12 z 26 liter.

Wiadomo było, że w równaniach 2.1 H jest identycznością. Nieznane natomiast było nastawienie bębenka N. Uwzględniając te informacje zapisano równania ponownie, ale w zmienionej formie:

$$\begin{aligned}
&Q = P^{-x}NP^{x}SA_1S^{-1}P^{-x}P^{-1}N^{-1}P^{x},\\
&Q = P^{-x-1}NP^{x+1}SA_2S^{-1}P^{-x-1}P^{-1}N^{-1}P^{x+1},\\
&\vdots\\
&Q = P^{-x-5}NP^{x+5}SA_6S^{-1}P^{-x-5}P^{-1}N^{-1}P^{x+5},
\end{aligned}$$

gdzie, tak jak poprzednio $Q = M^{-1}L^{-1}RLM$, a $x = 1, \ldots, 26$.
Gdyby także S była tożsamością, to powyższe równania przyjęłyby postać:

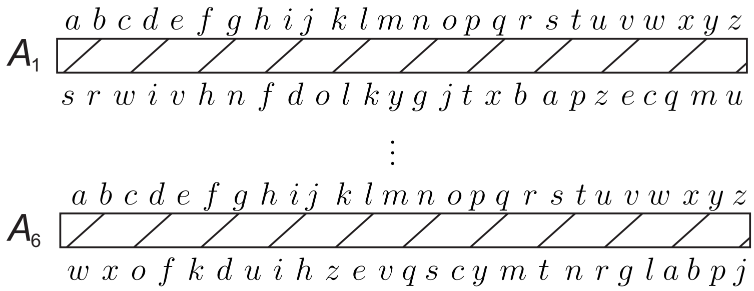
$$\begin{aligned}
&Q = P^{-x}NP^{x}A_1P^{-x}P^{-1}N^{-1}P^{x},\\
&Q = P^{-x-1}NP^{x+1}A_2P^{-x-1}P^{-1}N^{-1}P^{x+1},\\
&\vdots\\
&Q = P^{-x-5}NP^{x+5}A_6P^{-x-5}P^{-1}N^{-1}P^{x+5}.
\end{aligned}$$

Wtedy podstawiając za x kolejne liczby od 1 do 26, a następnie obliczając prawe strony, otrzymano by dla określonego x rozwiązanie Q, jednakowe dla wszystkich sześciu równań. W ten sposób poznano by również pozycję początkową wirnika N. Ponieważ jednak S nie była tożsamością, wyrażenia nie były równe. Były natomiast między nimi pewne podobieństwa. Do łatwiejszego, niż wykonywanie obliczeń, wyszukiwania wspólnych cech służyła właśnie metoda rusztu.

Na odpowiednio dużym arkuszu papieru wypisano, dla każdego z trzech bębenków, 31 permutacji: N, $P^{-1}NP, \ldots, P^{-25}NP^{25}$, N, $P^{-1}NP$, $P^{-2}NP^2$, $P^{-3}NP^3$, $P^{-4}NP^4$, w następujący sposób:

$$\begin{array}{ll}
N & k\,j\,p\,z\,y\,d\,t\,i\,o\,h\,x\,c\,s\,g\,u\,b\,r\,n\,w\,f\,m\,v\,e\,q\,l\,a \\
P^{-1}NP & i\,o\,y\,x\,c\,s\,h\,n\,g\,w\,b\,r\,f\,t\,a\,q\,m\,v\,e\,l\,u\,d\,p\,k\,z\,j \\
P^{-2}NP^2 & n\,x\,w\,b\,r\,g\,m\,f\,v\,a\,q\,e\,s\,z\,p\,l\,u\,d\,k\,t\,c\,o\,j\,y\,i\,h \\
\vdots & \vdots \\
P^{-4}NP^4 & u\,z\,p\,e\,k\,d\,t\,y\,o\,c\,q\,x\,n\,j\,s\,b\,i\,r\,a\,m\,h\,w\,g\,f\,l\,v.
\end{array}$$

Pierwsze sześć wyrażeń odpowiadało równaniom dla $x = 26$. Permutacje od $P^{-1}NP$ do $P^{-6}NP^6$ były dla $x = 1$, od $P^{-2}NP^2$ do $P^{-7}NP^7$ dla $x = 2$ itd. Ostatnie sześć iloczynów oznaczało pozycję $x = 25$. Następnie na ruszcie, czyli karcie z sześcioma otworami, wypisano permutacje A_i.



Przesuwając ruszt nad kartką z permutacjami $P^{-i}NP^i$ (i=1, ..., 26) szukano pozycji, w której wyrażenia na Q w każdym z sześciu równań były podobne. Następnie argumenty i litery obrazu w $A_1, \ldots, A_6$ należało pozamieniać miejscami w taki sposób, aby uzyskać identyczne Q. Dzięki tej metodzie uzyskiwano jednocześnie permutację S oraz nastawienie wirnika N. Nie był to jednak koniec pracy. Znając Q należało jeszcze rozwiązać równanie:

$$Q = P^{-y}M^{-1}P^{y}P^{-z}L^{-1}P^{z}RP^{-z}LP^{z}P^{-y}MP^{y}, \tag{4.1}$$

gdzie y i z były nieznanymi pozycjami początkowymi bębenków M i L odpowiednio. Połączenia M, L i R były wiadome. Podobnie jak x, y i z mogły przyjmować wartości od 1 do 26. Metoda, którą kryptolodzy stosowali do ich odnalezienia, polegała na ręcznej zmianie pozycji bębenków i próbie czytania depesz. Była to praca monotonna, ponieważ w najgorszej sytuacji należało sprawdzić $26^2 = 676$ przypadków. Po odnalezieniu pozycji startowej bębenków pozostawało jeszcze określić ustawienie pierścieni względem wirników. Szyfranci ustawiali je korzystając z miesięcznych tabeli kluczy dziennych. Polscy deszyfranci wykorzystywali natomiast w tym celu tzw. metodę ANX.

Dzięki odczytanym wiadomościom z września i października 1932 roku, wiadomo było kryptologom, że większość depesz rozpoczynała się od formuły „anx". Słowo „an" oznaczało niemieckie „do", a „x" było znakiem przestankowym. Żeby znaleźć szukane ustawienie pierścieni należało wybrać wiadomość, która w oparciu o wzór 2.1 mogła jako tekst jawny rozpoczynać się od litery a. Był to na przykład szyfrogram o początku tuv. Teraz naciskając klawisz t należało obracać bębenki do momentu, w którym zaświeciła się żarówka podświetlająca a. Następnie trzeba było nacisnąć klawisz u. Jeśli zapaliła się lampka n sprawdzano czy po wciśnięciu v zaświeci się x. Jeśli odpowiedź była pozytywna, wtedy z dużym prawdopodobieństwem dane ustawienie było prawidłowe. Pozostało już tylko przestawić pierścienie tak, aby litery widoczne w górnej części maszyny zgadzały się z kluczem dziennym. Jeżeli natomiast x nie powstało z v należało kontynuować postępowanie. Mimo że w niekorzystnym przypadku do sprawdzenia było $26^3 = 17576$ ustawień, była to metoda niezawodna.

4.2 Metoda zegara

W 1933 roku, widząc wyniki jakie odniósł Marian Rejewski w pracy nad rozkodowaniem Enigmy, zwierzchnicy zwiększyli liczbę osób deszyfrujących wiadomości. Do ścisłej pomocy Rejewskiemu przydzielono natomiast Jerzego Różyckiego oraz Henryka Zygalskiego, którzy wcześniej zajmowali się innymi szyframi. Głównym zadaniem kryptologów było rozkodowywanie kluczy dziennych i dostarczanie ich deszyfrantom. Ponieważ Niemcy do 1935 roku nie wprowadzili ważniejszych zmian w maszynie, trzej matematycy mogli także doskonalić techniki dekryptażu. Na początku sporządzili katalog permutacji Q według wzoru (4.1) dla sześciu możliwych położeń bębenków. Aby odczytać nastawienie wirników L i M należało najpierw wyznaczyć metodą rusztu pozycję wirnika N, a następnie znaleźć uzyskaną permutację Q w ka-

talogu. Odpowiadające jej ustawienie bębenków L i M było zamieszczone obok.

Na początku stosowania Enigmy kolejność wirników w maszynie była zmieniana tylko raz na trzy miesiące, ale już od lutego 1936 roku następowało to każdego miesiąca, a od października 1936 roku codziennie. Ważne więc stało się sprawne określanie, który wirnik znajdował się na szybkiej pozycji, czyli na pozycji bębenka N. Służyła do tego wynaleziona przez Różyckiego metoda zegara. Punktem wyjścia do jej opracowania był błąd konstruktorów Enigmy, którzy umieścili przy każdym pierścieniu zaczep. Powodował on obrót kolejnego bębenka o jedną pozycję, co miało uczynić ruch wirników bardziej nieregularnym. Umocowanie zaczepu w każdym wirniku przy innej literze było podstawą przy ustalaniu tożsamości szybkiego wirnika. Bębenek I powodował obrót kolejnego przy zmianie litery Q na R, bębenek II przy przejściu z E na F, a III przy obrocie V na W. Metoda zegara wykorzystywała także statystyczną własność języka polegającą na nierównej częstości występowania liter. Jeżeli bowiem napiszemy dwa teksty niemieckie jeden pod drugim, np.:

ESDUERFENALSOKEINECHIFFRIERVERFAHRENVERWENDETWERDE
KLARTELEGRAMMESINDINNORMALERSPRACHEABGEFASSTCODETE

to w obrębie 50 znaków, 5 liter w pionie będzie takich samych (teoretyczna wartość dla języka niemieckiego wynosi 8%). Szyfrując wiadomości według tego samego klucza depeszy własność ta zostanie zachowana. Jeżeli natomiast użyte zostaną dwa różne klucze, powtórzą się przeciętnie dwa znaki.

Posiadając dostateczną liczbę wiadomości z danego dnia, kryptolodzy potrafili określić, które z nich zostały zaszyfrowane takim samym kluczem. Do analizy wybierano te depesze, których klucze różniły się tylko trzecią literą, np.: *cce* i *cch*, *zda* i *zdr* itd. W takim przypadku można je było sprowadzić do pozycji, w której ich fragmenty zostały zakodowane z identycznego nastawienia wirników. Podczas szyfrowania telegramów liczących kilkadziesiąt znaków musiał nastąpić obrót środkowego wirnika. Należało więc określić przy której literze wirnika N miał miejsce przeskok bębenka M. Wykorzystywano do tego odpowiednie wiadomości. Jeśli klucze wybranych depesz różniły się o 7 znaków, należało dokonać przesunięcia tekstu o taką samą liczbę liter. Można to było zrobić na dwa sposoby: pierwszą umieścić 7 miejsc przed lub za drugą. Jeżeli ilość powtarzających się liter, w jednym z dwóch położeń, wynosiła w stosunku do całego tekstu co najmniej 8%, przesunięcie było prawidłowe. W przeciwnym przypadku należało szukać kolejnych depesz i podobieństw

występujących między nimi.

Przykład. Weźmy powyższy tekst w języku niemieckim. Zaszyfrujemy oba wersy. Najpierw użyjemy tego samego klucza (*aaa*), a następnie dwóch różnych (*aaa* i *aah*).

```
FXJRRTDYVTOAPJSKMZVQGCDGXZSIXMNGNBZPOQFSWTWKWHNTWV
WEZUXNUYYXKNXBEKMMDZBDKDFYXXFGCGVSZLLXNHXAYMOCKCOV
```

```
FXJRRTDYVTOAPJSKMZVQGCDGXZSIXMNGNBZPOQFSWTWKWHNTWV
ZATVELYSHPLLYYIVQVBZFJMLGOXLJHUHXKUHZLTXHPXBWBGYVC
```

W pierwszym przypadku liczba i miejsce występowania identycznych liter nie uległy zmianie. W drugiej sytuacji własność ta nie została zachowana. Powtórzenie się tylko jednej litery odpowiada przypadkowemu ciągowi znaków. Ponieważ użyte klucze różnią się o 7 liter, można przesunąć wiadomości względem siebie na dwa sposoby.

```
FXJRRTDYVTOAPJSKMZVQGCDGXZSIXMNGNBZPOQFSWTWKWHNTWV
       ZATVELYSHPLLYYIVQVBZFJMLGOXLJHUHXKUHZLTXHPXBWBGYVC
```

```
       FXJRRTDYVTOAPJSKMZVQGCDGXZSIXMNGNBZPOQFSWTWKWHNTWV
ZATVELYSHPLLYYIVQVBZFJMLGOXLJHUHXKUHZLTXHPXBWBGYVC
```

W pierwszej sytuacji powtarzają się 4 znaki, a w drugiej tylko 1. Właściwe jest więc ułożenie pierwszych dwóch wierszy. Jednocześnie widać, że podczas szyfrowania pierwszych ośmiu liter depeszy o kluczu *aaa*, nie nastąpił przeskok bębenka M. Wiemy więc, że na pozycji szybkiego wirnika nie został użyty II mechanizm. Gdyby tak było, porównywanie liter w pionie w dwóch tekstach nie dałoby wyniku 8%. Otrzymalibyśmy zwykłą mieszaninę znaków. Porównując kolejne telegramy eliminujemy pozostałe wirniki.

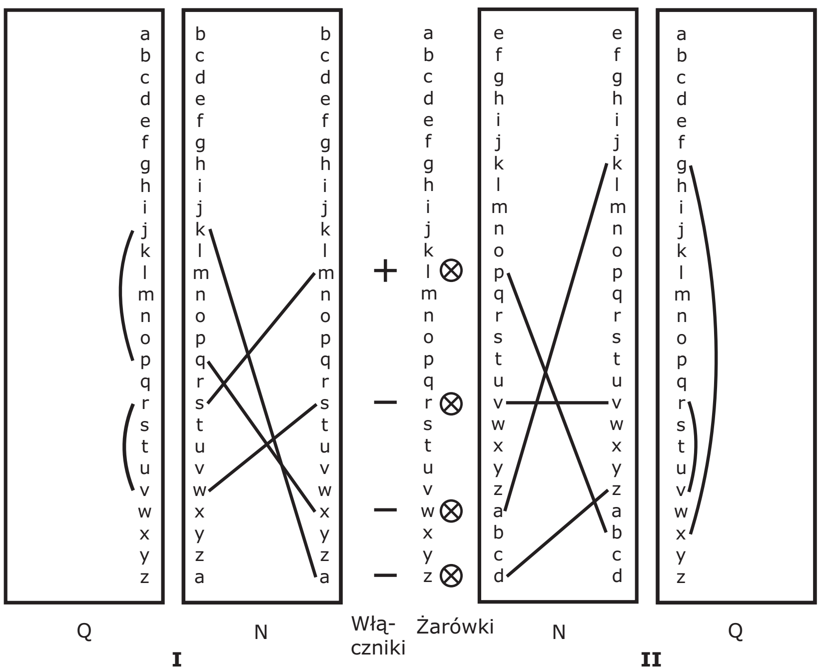
W każdym z trzech bębenków stosowanych na początku, zaczep umieszczony był w innym miejscu, co pozwalało jednoznacznie określić wirnik zajmujący położenie N. Wprowadzone później wirniki IV i V miały zaczepy umieszczone przy literach K i A odpowiednio. Dopiero przy włączaniu do użycia kolejnych trzech, kostruktorzy zauważyli swój błąd i umocowali w nowych wirnikach zaczepy w tym samym miejscu.

Metoda zegara wymyślona przez Jerzego Różyckiego, jako jedyna oparta była na lingwistycznych właściwościach języka niemieckiego. Wszystkie

pozostałe, opracowane przez polskich kryptologów, wykorzystywały matematyczną teorię i opierały się na obliczeniach.

4.3 Cyklometr

Wraz z upływem czasu coraz więcej niemieckich formacji wojskowych korzystało z Enigmy. Już 1 sierpnia 1935 roku lotnictwo zaczęło posługiwać się maszyną wojskową, wykorzystując jednak własne klucze dzienne. Dołączanie nowych jednostek powodowało, że Polacy musieli odtwarzać rosnącą liczbę kluczy dziennych. Ponadto, oprócz codziennej zamiany bębenków, Niemcy od 1 października 1936 roku zmieniali od 5 do 8 par liter na łącznicy. Modyfikacje te sprawiały, że posługiwanie się metodą rusztu było uciążliwe. Należało znaleźć nowe sposoby ułatwiające pracę.



Rysunek 4.1: Schemat działania cyklometru.

Pomysł, który się zrodził wykorzystywał kształt iloczynów:

$$A_4A_1 = S^{-1}P^{-4}N^{-1}P^4QP^{-4}NP^3N^{-1}PQP^{-1}NPS,$$
$$A_5A_2 = S^{-1}P^{-5}N^{-1}P^5QP^{-5}NP^3N^{-1}P^2QP^{-2}NP^2S,$$
$$A_6A_3 = S^{-1}P^{-6}N^{-1}P^6QP^{-6}NP^3N^{-1}P^3QP^{-3}NP^3S.$$

Permutacja S nie miała wpływu na długość cykli w iloczynach, a jedynie na występujące w nich litery. Postać charakterystyk powtarzała się więc rzadko i mogła być traktowana jako określająca konkretny dzień. Porównanie struktury charakterystyk danego dnia ze skatalogowanymi, dałoby w przeciągu kilkunastu minut szukane ustawienie bębenków. Do opracowania potrzebnego katalogu posłużył właśnie cyklometr.

Składał się on z dwóch zestawów bębenków Enigmy wojskowej oraz zestawu 26-ciu żarówek i przełączników. Szybki wirnik II-giej części urządzenia przesunięty był o 3 pozycje do przodu, względem mechanizmu N części I-szej. Takie ustawienie stwarzało sytuację, która miałaby miejsce po jednokrotnym zaszyfrowaniu klucza, czyli po przeskoku szybkiego wirnika o trzy znaki.

Po włączeniu prądu przy wybranej literze (znak „+” na rysunku 4.1), prąd płynął przez bębenki N, M, L i R części I-szej oraz części II-giej maszyny (mechanizmom M, L i R na schemacie odpowiada wirnik Q). Jednocześnie zapalały się żarówki przy wszystkich literach wchodzących do danego cyklu i do drugiego cyklu tej samej pary iloczynu A_4A_1. Po zanotowaniu liczby świecących się żarówek, włączano przełącznik przy literze, która nie weszła do poprzednich cykli i kontynuowano postępowanie do wyczerpania wszystkich liter alfabetu. Następnie przestawiano wirniki N urządzenia o jedną pozycję i notowano liczbę znaków w cyklach permutacji A_5A_2. To samo postępowanie powtarzano także dla A_6A_3. Dla czytelniejszego opisu, a także łatwości wyszukiwania pozycji z katalogu, każdej strukturze przypisano numer.

Liczba porządkowa	Postać iloczynu $A_{i+3}A_i$
1	(13)(13)
2	(12)(12)(1)(1)
3	(11)(11)(2)(2)
4	(11)(11)(1)(1)(1)(1)
⋮	⋮
101	$\underbrace{(1)(1)(1)(1)\ldots(1)(1)}_{26\ razy}$

Po sporządzeniu katalogu dla 6-ciu możliwych ustawień bębenków, cyklometr schowano i korzystano tylko z kartek katalogu, uporządkowanych według długości cykli. Każda z pozycji była podobna do przedstawionej:

GHT – (15, 12, 87).

Litery GHT oznaczały ustawienie wirników dla charakterystyk postaci:

A_4A_1 forma nr 15,
A_5A_2 forma nr 12,
A_6A_3 forma nr 87.

Iloczyny odtworzone danego dnia z przechwyconych depesz porównywano z opisanymi, otrzymując pozycje wirników. Z pudełka, w którym przechowywano kartę, odczytywano kolejność bębenków. Pozycję pierścieni wewnętrznych uzyskiwano stosując metodę ANX. Znaki zamienione przez łącznicę S odtwarzano porównując litery wystukane na maszynie z literami w charakterystykach danego dnia. Dysponując takim katalogiem kryptolodzy przekazywali deszyfrantom klucz dzienny w ciągu kilkunastu minut.

Praca nad stworzeniem katalogu trwała ponad rok, ponieważ do opisania było $26^3 = 17576$ pozycji bębenków dla każdego z 6-ciu możliwych ustawień wirników. Ponadto kryptolodzy musieli codziennie odnajdywać bieżące klucze dzienne posługując się metodą rusztu. 2 listopada 1937 roku Niemcy zamienili dotychczasowy bębenek odwracający na nowy, co uczyniło opracowany katalog bezużytecznym. Kryptolodzy musieli więc odtworzyć połączenia zamienionego wirnika oraz opracować katalog cykli na nowo.

5 Bomba Rejewskiego i płachty Zygalskiego

Wszystkie dotychczas wynalezione metody odtwarzania kluczy dziennych przestały być użyteczne 15 września 1938 roku. Z tym dniem Niemcy zmienili przepisy dotyczące szyfrowania depesz. Tak jak poprzednio sprawdzano, które wirniki i w jakiej kolejności należy użyć oraz jak ustawić pierścienie wewnętrzne. Nie obowiązywało już jednak ustalone z góry nastawienie początkowe wirników. Szyfrant samodzielnie wybierał dla każdej depeszy pozycje bębenków, które zamieszczał klerem w nagłówku wiadomości. Następnie przestawiał wirniki na podane litery i dwukrotnie kodował wybrany indywidualnie klucz depeszy. Otrzymanych sześć liter umieszczał na początku szyfrogramu, po czym ponownie zmieniał nastawienie wirników według klucza depeszy i dopiero z tej pozycji szyfrował właściwy przekaz. Klucz depeszy składał się więc teraz z dziewięciu znaków, np.: *shp*, *chv pzt*. Ze względu na różne dla każdej depeszy trzy pierwsze litery, nie istniały już charakterystyki dnia w postaci iloczynów A_4A_1, A_5A_2 i A_6A_3. Zauważono jednak, że około 40% zakodowanych kluczy jest postaci *pst pwa* (*abq kbe*, *pgr dnr*). Oznaczało to, że istnieją punkty stałe niezależne od permutacji S. Własność tą wykorzystano do stworzenia katalogu punktów stałych, dla wszystkich 17576 pozycji dla każdej z sześciu możliwych kolejności wirników.

5.1 Bomba Rejewskiego

Pierwszym urządzeniem, które skonstruowano, a którego zasada działania wykorzystywała fakt istnienia w kluczach punktów stałych, była tzw. bomba Rejewskiego. Składała się ona z zestawu bębenków sześciu Enigm połączonych parami, przy czym wirnik N drugiej Enigmy w każdej parze był przesunięty o trzy pozycje do przodu względem szybkiego wirnika pierwszej maszyny. Takie ustawienie odpowiadało sytuacji po jednokrotnym zakodowaniu klucza. Bomba szukała położeń wirników, w których występowały punkty stałe na pierwszej i czwartej, drugiej i piątej oraz trzeciej i szóstej pozycji jednocześnie. Ponieważ zarówno kolejność wirników na osi maszyny jak i ustawienie pierścieni były niewiadome, więc sama znajomość punktu stałego nie wystarczała do odtworzenia klucza wiadomości. Do odnalezienia ustawienia bębenków wykorzystywano odległości względne pomiędzy ustawieniem wirników (podanym jawnie), a miejscem w którym wystąpi samiczka.

Przystępując do szukania ustawień wirników należało najpierw znaleźć

szyfrogramy, w których punktem stałym była ta sama litera.

Ustawienie bębenków	Klucz wiadomości
rtj	*wah wik*
dqx	*dwj mwr*
hpl	*raw ktw*

Następnie wprowadzono oznaczenia:

W_{11} – ustawienie bębenka N przed szyfrowaniem pierwszego klucza;
W_{12} – ustawienie bębenka N przed szyfrowaniem drugiego klucza;
W_{13} – ustawienie bębenka N przed szyfrowaniem trzeciego klucza;
$W_{ij} + p$ – położenie i-tego bębenka po zakodowaniu p znaków j-tej wiadomości.

Z dostępnych kluczy wynikało, że litera w była otrzymywana dla:

$$\begin{array}{ccc} W_{11} & \text{i} & W_{11} + 3, \\ W_{12} + 1 & \text{i} & W_{12} + 4, \\ W_{13} + 2 & \text{i} & W_{13} + 5. \end{array} \tag{5.1}$$

Z podanego klucza Enigmy można było także obliczyć względne odległości pomiędzy wirnikami. Przed szyfrowaniem pierwszej litery klucza pierwszej wiadomości, wirnik N znajdował się w pozycji j. Podczas kodowania drugiej depeszy był ustawiony na literę x. Względna odległość pomiędzy tymi dwoma położeniami wynosi 14 znaków. Podobnie przy szyfrowaniu drugiego i trzeciego telegramu względny dystans dzielący ustawienie wirników (x i l) jest równy 14. Można zapisać dwa równania:

$$\begin{array}{l} W_{12} = W_{11} + 14, \\ W_{13} = W_{12} + 14. \end{array} \tag{5.2}$$

Podstawiając zależności 5.2 do 5.1 ustalano w jakim położeniu wyjściowym wirników otrzymywano literę w:

$$
\begin{array}{lcl}
W_{11} & \text{oraz} & W_{11}+3, \\
W_{11}+15 & \text{oraz} & W_{11}+18, \\
W_{11}+4 & \text{oraz} & W_{11}+7.
\end{array}
$$

Dzięki powyższym związkom wiadomo było w jaki sposób ustawić bębenki bomby, aby znaleźć ustawienie wirników generujące punkty stałe.

1. W pierwszej parze Enigm wirnik N pierwszego urządzenia ustawiano w dowolnej pozycji, a w drugim urządzeniu przestawiano o trzy znaki do przodu względem pierwszej maszyny.
2. Wirnik N pierwszej Enigmy w drugiej parze przestawiano o 15 pozycji względem tego samego bębenka w pierwszej parze. Szybki wirnik w drugim urządzeniu, ustawiano 3 znaki do przodu względem pierwszej maszyny tej samej pary.
3. Szybki bębenek pierwszego urządzenia trzeciej pary należało przestawić 4 litery do przodu w stosunku do szybkiego wirnika pierwszej maszyny w pierwszej parze. Z wirnikiem N w drugiej maszynie postępowano tak jak w pierwszej i drugiej parze Enigm.
4. Wirniki M i L w drugiej i trzeciej parze ustawiano bazując na odległościach między poszczególnymi literami odpowiednich kluczy. Odległość pomiędzy literą t w kluczu pierwszej depeszy, a literą q w kluczu drugiej wynosi 23. O taką liczbę znaków należało więc przestawić środkowe wirniki w drugiej parze maszyn względem bębenków M pierwszej pary. Wirniki L w drugiej parze przestawiano o 12 znaków (dystans między r i d) w stosunku do wolnych bębenków pierwszej pary. Podobnie obliczano pozycje, w których należało ustawić mechanizmy M i L w trzeciej parze Enigm.

Po ustawieniu wirników włączano bombę, która zatrzymywała się w momencie wykrycia litery w jednocześnie w każdej z trzech par urządzeń. Osoba obsługująca maszynę zapisywała pozycję wirników w której to nastąpiło i powtórnie ją uruchamiała. Zmiana kolejności bębenków, po zakończeniu pracy przy jednym z ustawień, i ponowne włączenie urządzenia znacznie wydłużyłoby czas oczekiwania na możliwe rozwiązania. Skonstruowano więc sześć bomb, po jednej dla każdej z możliwych kolejności wirników na osi maszyny. W ciągu dwóch godzin urządzenia dostarczały wszystkie prawdopodobne pozycje wirników, które należało sprawdzić odczytując fragment depeszy.

Do ustalenia pozostały jeszcze kryptologom ustawienia pierścieni i łącznicy. Właściwe pozycje pierścieni znajdowano manewrując nimi, przy ustalonym wcześniej nastawieniu bębenków, do momentu podświetlenia liter *rtj* przy jednoczesnym wystukiwaniu *wah wik*. Odnalezienie połączeń łącznicy polegało w pierwszym kroku na usunięciu przewodów. Następnie próbowano odczytać tekst dowolnej wiadomości. Otrzymywano zniekształcony tekst, np.:

RRRBISMCVAKCCCDIEFLOTTE.

Litery RRR musiały oznaczać litery VVV, czyli powtórzony skrót od niemieckiego „von" oznaczającego nadawcę. Podobnie CCC znaczyły AAA od słowa „an" oznaczającego odbiorcę. Połączywszy odpowiednie pary znaków na łącznicy wtyczkowej, można już było odczytać tekst bez błędów:

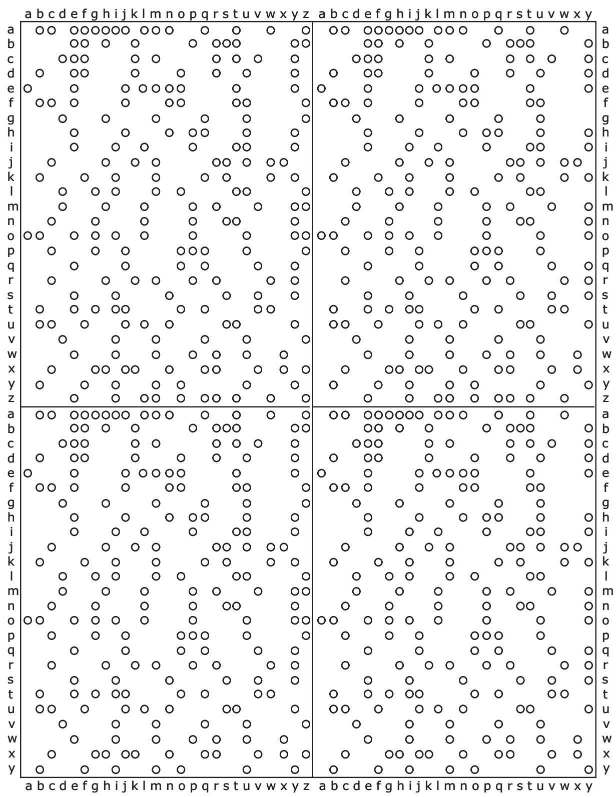
VVVBISMARCKAAADIEFLOTTE.

Na podstawie dalszej części wiadomości dowódcy pancernika Bismarck, należało zamienić pozostałe litery.

Mimo ułatwień jakie niosło ze sobą skonstruowanie bomby, miała ona także słabe strony. Pierwszą było przypuszczenie dotyczące zachowania pozycji przez środkowy wirnik. Podczas korzystania z maszyny trzeba było przyjąć, że nie nastąpiło przesunięcie bębenka M w trakcie szyfrowania klucza depeszy. Drugą wadą użytkowania urządzenia było założenie, że szukana litera nie została zamieniona przez łącznicę wtyczkową. Do stycznia 1939 roku permutacja S przekształcała jednak od 5 do 8 par liter. Można więc było przyjąć, że w przynajmniej 50% przypadków, S pozostawi bez zmian literę występującą w kluczach trzech wiadomości po dwa razy. Przy zwiększeniu liczby połączeń łącznicy do 10, taki przypadek zachodził rzadko. Wprowadzenie przez Niemców dwóch dodatkowych walców także nie pozostało bez wpływu na pracę kryptologów. Dzięki SD, formacji wojskowej utworzonej w 1937 roku, która szyfrowała wiadomości według starych zasad, udało się odtworzyć połączenia wewnętrzne IV i V walca. Zbudowanie jednak 60-ciu układów dla 5-ciu walców wykraczało poza możliwości techniczne Biura Szyfrów.

5.2 Płachty Zygalskiego

Drugi pomysł wykorzystania punktów stałych, do odszukiwania dziennych ustawień Enigmy, powstał w tym samym czasie co idea bomb. Henryk Zygalski zaproponował, aby wykorzystać fakt powtarzania się dowolnej litery zaszyfrowanego klucza do stworzenia katalogu. Dzięki niemu można by było porównać cykle jednoliterowe z kluczy depesz, z opisanymi przy znanym ustawieniu pierścieni i bębenków. Ponieważ przy nowym sposobie szyfrowania pozycje wirników były jawne, nie znane natomiast było ustawienie pierścieni oraz kolejność bębenków, należało wykorzystać względną odległość między punktami stałymi klucza. Korzystając z tych zależności wyliczano niewiadome posługując się płachtami perforowanymi.



Rysunek 5.1: Płachta Zygalskiego.

Komplet płacht składał się z 26-ciu arkuszy papieru oznaczonych od A do Z (26 możliwych położeń bębenka L). Posługiwanie się płachtami wymagało ich przesuwania względem siebie. Aby więc część pozycji nie wypadła z obserwacji, na każdym arkuszu narysowano cztery prostokąty, których krawędzie opisano literami alfabetu od a do z i od a do y. Odcięte i rzędne odpowiadały pozycjom wirników M i N, a ich przecięcie odpowiednim permutacjom. Jeśli w danym położeniu bębenków występował cykl jednoliterowy, odpowiednie pole perforowano.

Przed użyciem płacht trzeba było wybrać wiadomości o kluczach, w których punkt stały znajdował się na pierwszym i czwartym miejscu. Następnie należało przyjąć założenie dotyczące kolejności wirników na osi maszyny (np. 132) i ustawienia pierścieni w pierwszym kroku (QZZ). Przyjęto oznaczenia:

r_i – nastawienie pierścienia i-tego bębenka;

o_i – ustawienie początkowe i-tego wirnika;

t_i – litera, przy której ma miejsce obrót i-tego mechanizmu.

Wyliczając

$$q = t_1 - o_1 - 1\,(mod 26),$$

można było wyeliminować te depesze, w których podczas kodowania klucza doszło do obrotu środkowego wirnika, czyli spełniające warunek:

$$\mathrm{E}\Big(\frac{j-q+26}{26}\Big) \neq 0, \quad j = 0, \ldots, 5.$$

Używanie płacht miało na celu zweryfikowanie poprawności założeń dotyczących kolejności bębenków i ustawienia pierścienia L. Załóżmy, że po przeprowadzeniu obliczeń pozostały między innymi, takie klucze np.:

$$\begin{array}{rl} ptj, & \underline{x}zi\ \underline{x}pg; \\ ceh, & \underline{c}ms\ \underline{c}id; \\ bug, & \underline{r}cj\ \underline{r}vu; \\ bsu, & \underline{a}qy\ \underline{a}fk. \end{array}$$

Najpierw wybierano pierwszy klucz ptj i odpowiadający mu arkusz. Następnie kartę odpowiadającą ceh, układano w taki sposób, aby punkt o współrzędnych (h, e) pokrył się z (j, t) z poprzedniej płachty. Odpowiadało to przesunięciu w wierszach i kolumnach:

$$s_v = \mathrm{j} - \mathrm{h} = 10 - 8 = 2 = \mathrm{b},$$
$$s_c = \mathrm{t} - \mathrm{e} = 20 - 5 = 15 = \mathrm{o}.$$

Daną płachtę należało więc umieścić w punkcie o współrzędnych (b, o). Indykator *ceh* odpowiadał też nowemu ustawieniu pierścieni bębenków M i N. Odległość względna między literą h i pozycją pierścienia N musiała się równać 16 (liczba znaków oddzielających j i Z). Podobnie dystans między e i pozycją M wynosił 6 (odległość między t i Z), stąd:

$$r_1 = \mathrm{X} \quad \text{oraz} \quad r_2 = \mathrm{K}.$$

Po nałożeniu na siebie około dwunastu arkuszy procedurę zakańczano.

Jeśli pozostał widoczny jeden otwór o współrzędnych np. (d, j), było to właściwe rozwiązanie. Ze względu na przesunięcie punktu w stosunku do założonej pozycji pierścieni, trzeba było jeszcze wyliczyć ich poprawne ustawienie:

$$r_1 = \mathrm{j} - \mathrm{d} = \mathrm{F},$$
$$r_2 = \mathrm{t} - \mathrm{j} = \mathrm{J}.$$

Właściwą kolejnością bębenków na osi było więc 132, a ustawieniem pierścieni QJF. Permutację S wyznaczano natomiast porównując litery klucza z wystukanymi na Enigmie.

W przypadku gdy uzyskano kilka prawdopodobnych rozwiązań, należało sprawdzić każde z nich na fragmencie depeszy. Jeżeli natomiast żaden otwór nie przeświecał przez karty oznaczało to, że badana hipoteza była błędna i należy powtórzyć rozumowanie dla innych wartości. W najgorszym przypadku do sprawdzenia było 156 założeń (po 26 pozycji bębenka L dla 6 ustawień wirników na osi).

Każdy z 6-ciu wykonanych kompletów płacht zawierał 26 arkuszy. W każdej karcie należało wyciąć około tysiąca otworów, ponieważ punkt stały trzeba było zaznaczyć nawet czterokrotnie. Ze względu na ilość wymaganej pracy, do 15 grudnia 1938 roku zostały wykonane tylko dwa zestawy. Wtedy Niemcy zaczęli używać dodatkowe dwa bębenki szyfrujące. Wykonanie brakujących 58-miu kompletów, przekraczało możliwości trzech kryptologów. Dopiero po wybuchu wojny Anglicy sporządzili wszystkie potrzebne arkusze perforowane i dostarczyli je Polakom do Francji.

Literatura

[1] Zbigniew Błocki, *Matematyczne aspekty rozszyfrowania Enigmy.* Wykład habilitacyjny na Wydziale Matematyki, Fizyki i Informatyki, Kraków 2001.

[2] Marek Grajek, *Enigma: bliżej prawdy.* Rebis, Poznań 2007.

[3] Władysław Kozaczuk, *W kręgu Enigmy.* Książka i Wiedza, Warszawa 1979.

[4] Marian Rejewski, *Wiadomości matematyczne XXIII.*

[5] Marian Rejewski, *Applicationes mathematicae XVI.*

[6] Marian Rejewski, *1930-1940 Metoda i historia rozwiązania niemieckiego szyfru maszynowego.* Ze zbiorów Władysława Kozaczuka.

[7] Marian Rejewski, *Rejewski o płachtach Zygalskiego.* Ze zbiorów Władysława Kozaczuka.

[8] Jerzy Rutkowski, *Algebra abstrakcyjna w zadaniach.* Wydawnictwo Naukowe PWN, Warszawa 2002.

[9] Tony Sale, *The Breaking of Enigma by the Polish Mathematicians.* Virtual Bletchley Park website.